

BEST AVAILABLE COPY

Method for providing postal items with postal prepayment impressions

Patent number: DE10020566
Publication date: 2001-10-31
Inventor: MEYER BERND (DE); LANG JUERGEN (DE)
Applicant: DEUTSCHE POST AG (DE)
Classification:
 - **international:** G07B17/00; G07B17/00; (IPC1-7): G07B17/04;
 H04L9/28
 - **european:** G07B17/00D2
Application number: DE20001020566 20000427
Priority number(s): DE20001020566 20000427

Also published as:
 WO 0182233 (A1)
 US 2004028233 (A1)
 CA 2428676 (A1)

[Report a data error here](#)

Abstract of DE10020566

The invention relates to a method for providing postal items with postal prepayment impressions, characterized in that data are generated in the customer system that are encrypted in such a manner that the value transfer center is able to decrypt them. To this end, the data are transmitted from the customer system to the value transfer center. The value transfer center then decrypts the data and re-encrypts them with a code not known to the customer system and transmits the encrypted data to the customer system.

Security architecture

PC franking

1. Generating and storing a random number
2. Encrypting the random number and the ID number
3. Loading center
4. Decryption of random number and specification ID
5. Identification of the customer/customer system
6. Encryption of random number and of specification ID
7. Transmission of encrypted random number and specification ID

Customer system

"Safe Box" in the customer system

8. Input of mailing data by the customer
9. Hash value on the basis of stored random number and mailing data
10. In the postage indicium:
 - mailing data in plain text
 - encrypted random number and specification ID as well as
 - hash value
11. Verification of mailing data, i.e. if mailing matches
12. Decryption of random number and of specification ID, i.e. validity of specification
13. Hash value from decrypted random number and mailing data
14. Comparison of the two hash values, i.e. real specification AND mailing data originate from Safe Box
15. Countercheck franking value against specification amounts

Data supplied from the **esp@cenet** database - Worldwide



Offenlegungsschrift

⑩ DE 100 20 566 A 1

⑯ Int. Cl. 7:

G 07 B 17/04

H 04 L 9/28

DE 100 20 566 A 1

⑯ Aktenzeichen: 100 20 566.6

⑯ Anmeldetag: 27. 4. 2000

⑯ Offenlegungstag: 31. 10. 2001

⑯ Anmelder:

Deutsche Post AG, 53175 Bonn, DE

⑯ Vertreter:

Jostarndt Thul Patentanwälte, 52076 Aachen

⑯ Erfinder:

Meyer, Bernd, 53639 Königswinter, DE; Lang, Jürgen, Dr., 51429 Bergisch Gladbach, DE

⑯ Entgegenhaltungen:

DE	197 44 913 A1
US	55 86 036
WO	98 14 907 A2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

⑯ Verfahren zum Versehen von Postsendungen mit Freimachungsvermerken

⑯ Die Erfindung betrifft ein Verfahren zum Versehen von

Postsendungen mit Freimachungsvermerken.
Erfindungsgemäß zeichnet sich das Verfahren dadurch aus, dass in dem Kundensystem Daten erzeugt werden, die so verschlüsselt sind, dass das Wertübertragungszentrum diese entschlüsseln kann, dass die Daten von dem Kundensystem zu dem Wertübertragungszentrum gesendet werden und dass das Wertübertragungszentrum gesendet werden und dass das Wertübertragungszentrum die Daten entschlüsselt und anschließend die Daten erneut mit einem dem Kundensystem nicht bekannten Schlüssel verschlüsselt und die so verschlüsselten Daten anschließend an das Kundensystem überträgt.

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Versehen von Postsendungen mit Freimachungsvermerken, wobei ein Kundensystem von einem Wertübertragungszentrum über eine Datenleitung einen Gebührenbetrag lädt, wobei das Kundensystem ein Drucken von Freimachungsvermerken auf Postsendungen steuert und wobei das Wertübertragungszentrum ein Datenpaket an das Kundensystem sendet.

[0002] Ein gattungsgemäßes Verfahren ist aus der internationalen Patentanmeldung WO 98 14907 bekannt.

[0003] Ein weiteres Verfahren ist aus der Deutschen Patentschrift DE 31 26 785 C2 bekannt. Bei diesem Verfahren erfolgt eine Erzeugung eines für eine Frankierung von Postsendungen bestimmten Nachladesignals in einem separaten Bereich eines von einem Postbeförderungsunternehmen betriebenen Wertübertragungszentrums.

[0004] Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zum Freimachen von Briefen zu schaffen, das sich sowohl zum Freimachen einzelner Briefe als auch zum Freimachen einer Vielzahl von Briefen eignet.

[0005] Erfindungsgemäß wird diese Aufgabe dadurch gelöst, dass in dem Kundensystem Daten erzeugt werden, die so verschlüsselt sind, dass das Wertübertragungszentrum diese entschlüsseln kann, dass die Daten von dem Kundensystem zu dem Wertübertragungszentrum gesendet werden und dass das Wertübertragungszentrum die Daten entschlüsselt und anschließend die Daten erneut mit einem dem Kundensystem nicht bekannten Schlüssel codiert und die so verschlüsselten Daten anschließend an das Kundensystem überträgt.

[0006] Das Kundensystem ist vorzugsweise so gestaltet, dass es nicht in der Lage ist, von dem Wertübertragungszentrum gesandte Daten vollständig zu entschlüsseln, jedoch ein Briefzentrum, in dem die Postsendungen auf eine korrekte Frankierung überprüft werden, diese Daten entschlüsseln kann.

[0007] Das Wertübertragungszentrum kann auf verschiedene Weisen gestaltet sein. Der Begriff Wertübertragungszentrum umfasst sowohl bekannte Wertübertragungszentren als auch neue Formen von Wertübertragungszentren.

[0008] Die Erfindung betrifft insbesondere solche Wertübertragungszentren, über die auf eine Datenkommunikationsleitung unmittelbar zugegriffen werden kann, wie an das Internet oder an Telefonleitungen angeschlossene Datenserver.

[0009] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass die Verschlüsselung in dem Kundensystem unter Einsatz einer Zufallszahl erfolgt.

[0010] Es ist zweckmäßig, dass die Zufallszahl in einem Sicherungsmodul erzeugt wird, auf das ein Benutzer des Kundensystems keinen Zugriff hat.

[0011] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass die Zufallszahl zusammen mit einem von dem Wertübertragungszentrum ausgegebenen Sitzungsschlüssel und einem öffentlichen Schlüssel des Wertübertragungszentrums verschlüsselt wird.

[0012] Es ist zweckmäßig, dass das Kundensystem die Daten mit einem privaten Schlüssel signiert.

[0013] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass der private Schlüssel in dem Sicherungsmodul gespeichert ist.

[0014] Es ist zweckmäßig, dass die Daten mit jeder Anforderung eines Gebührenbetrages von dem Kundensystem an das Wertübertragungszentrum übertragen werden.

[0015] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass das Wertübertragungszentrum anhand der übermittelten Daten das Kundensystem identifiziert.

[0016] Es ist zweckmäßig, dass das Wertübertragungszentrum die von ihm verschlüsselten Daten an das Kundensystem schickt.

[0017] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass die von dem Wertübertragungszentrum an das Kundensystem gesandten Daten einen ersten Bestandteil aufweisen, der von dem Kundensystem nicht entschlüsselt werden kann und dass die Daten ferner einen zweiten Anteil aufweisen, der von dem Kundensystem entschlüsselt werden kann.

[0018] Es ist zweckmäßig, dass der in dem Kundensystem entschlüsselbare Teil der Daten Informationen über die Identität des Kundensystems enthält.

[0019] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass der von dem Kundensystem entschlüsselbare Anteil der Daten Informationen über die Höhe eines Gebührenbetrages enthält.

[0020] Es ist zweckmäßig, dass ein Senden von Daten von dem Kundensystem an das Wertübertragungszentrum lediglich dann erfolgt, wenn in dem Kundensystem ein Betrag in einer Mindesthöhe geladen werden soll.

[0021] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass in dem Kundensystem ein Hash-Wert gebildet wird.

[0022] Es ist zweckmäßig, dass der Hash-Wert unter Einbeziehung von Angaben über Sendungsdaten gebildet wird.

[0023] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass der Hash-Wert unter Einbeziehung einer zwischengespeicherten Zufallszahl gebildet wird.

[0024] Es ist zweckmäßig, dass der Hash-Wert unter Einbeziehung einer Ladevorgangsidentifikationsnummer gebildet wird.

[0025] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass der Freimachungsvermerk logische Daten enthält.

[0026] Es ist zweckmäßig, dass der Freimachungsvermerk Informationen über Sendungsdaten enthält.

[0027] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass die logischen Daten Informationen über die verschlüsselte

Zufallszahl enthalten.

[0028] Es ist zweckmässig, dass die logischen Daten Informationen über die verschlüsselte Ladevorgangsidentifikationsnummer enthalten.

5

[0029] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass die logischen Daten Informationen über den Hash-Wert enthalten.

[0030] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass der Freimachungsvermerk sowohl von dem Wertübertragungszentrum übertragene Informationen als auch von dem Dokumenthersteller eingegebene Daten enthält.

10

[0031] Es ist zweckmässig, das Verfahren so durchzuführen, beziehungsweise das Kundensystem oder das Wertübertragungszentrum so auszustalten, dass der Freimachungsvermerk einen Hash-Wert enthält, der aus einer Kombination aus einem von dem Vorgabezentrum übertragenen Wert und von dem Dokumenthersteller eingegebenen Werten gebildet wird.

15

[0032] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass sie folgende Verfahrensschritte beinhalten: In dem Kundensystem oder in einem mit dem Kundensystem verbundenen Sicherungsmodul wird ein Geheimnis erzeugt und anschliessend zusammen mit Informationen über die Identität des Dokumentherstellers und/oder des von ihm eingesetzten Kundensystems an das Wertübertragungszentrum übermittelt.

15

[0033] Es ist zweckmässig, das Verfahren so durchzuführen, beziehungsweise das Kundensystem oder das Wertübertragungszentrum so auszustalten, dass das Wertübertragungszentrum die verschlüsselte Zusatzzahl entschlüsselt und wieder derart verschlüsselt, dass nur das Briefzentrum diese entschlüsseln kann und anschliessend eine Ladeidentifikationsnummer erzeugt.

20

[0034] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass bei der Erzeugung der Ladeidentifikationsnummer die verschlüsselte Zufallszahl eingeht.

25

[0035] Es ist zweckmässig, das Verfahren so durchzuführen, beziehungsweise das Kundensystem oder das Wertübertragungszentrum so auszustalten, dass die Ladeidentifikationsnummer an das Sicherungsmodul übertragen wird.

30

[0036] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass in dem Sicherungsmodul ein Hash-Wert aus der Ladeidentifikationsnummer und weiteren Daten gebildet wird.

35

[0037] Es ist zweckmässig, das Verfahren so durchzuführen, beziehungsweise das Kundensystem oder das Wertübertragungszentrum so auszustalten, dass der Freimachungsvermerk so erzeugt wird, dass er den Hash-Wert enthält.

40

[0038] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass die Gültigkeit von Freimachungsvermerken in dem Briefzentrum überprüft wird.

45

[0039] Es ist zweckmässig, das Verfahren so durchzuführen, beziehungsweise das Kundensystem oder das Wertübertragungszentrum so auszustalten, dass die Prüfung in dem Briefzentrum durch eine Analyse von in dem Freimachungsvermerk enthaltenen Daten erfolgt.

[0040] Eine vorteilhafte Ausführungsform des Verfahrens, eine bevorzugte Ausgestaltung des Kundensystems und des Wertübertragungszentrums zeichnen sich dadurch aus, dass die Prüfungsstelle aus in dem Freimachungsvermerk enthaltenen Daten einen Hash-Wert bildet und überprüft, ob dieser Hash-Wert mit einem in dem Freimachungsvermerk enthaltenen Hash-Wert übereinstimmt und im Falle der Nichtübereinstimmung den Freimachungsvermerk als gefälscht registriert.

[0041] Weitere Vorteile, Besonderheiten und zweckmässige Weiterbildungen der Erfindung ergeben sich aus der nachfolgenden Darstellung eines bevorzugten Ausführungsbeispiels anhand der Zeichnungen.

50

[0042] Von den Zeichnungen zeigt

[0043] Fig. 1 eine Prinzipdarstellung eines erfindungsgemäßen Verfahrens,

[0044] Fig. 2 die in Fig. 1 dargestellte Prinzipdarstellung mit einer Hervorhebung der bei einem Frankierungsvorgang beteiligten Parteien,

55

[0045] Fig. 3 Schnittstellen des in Fig. 1 und Fig. 2 dargestellten Frankierungssystems und

50

[0046] Fig. 4 eine Prinzipdarstellung von in dem Verfahren eingesetzten Sicherheitsmechanismen.

[0047] Das nachfolgende Ausführungsbeispiel beschreibt die Erfindung anhand eines vorgesehenen Einsatzes im Bereich der Deutschen Post AG. Es ist jedoch selbstverständlich gleichermaßen möglich, die Erfindung für eine Freimachung von anderen Dokumenten, insbesondere für einen Einsatz im Bereich von anderen Versandunternehmen, einzusetzen.

55

[0048] Die Erfindung stellt eine mögliche neue Form der Frankierung bereit, mit der Kunden unter Benutzung eines herkömmlichen PC mit Drucker und zusätzlicher Soft- und gegebenenfalls Hardware sowie eines Internet-Zugangs "digitale Freimachungsvermerke" auf Briefe, Postkarten etc. drucken können.

[0049] Eine Bezahlung zum Ausgleich des Wertes der von den Kunden ausgedruckten Frankierwerte kann auf verschiedene Weisen geschehen. Beispielsweise wird ein gespeichertes Guthaben verringert. Dieses Guthaben ist vorzugsweise digital gespeichert. Eine digitale Speicherung erfolgt beispielsweise auf einer speziellen Kundenkarte, einer standardisierten Geldkarte oder einem virtuellen Speicher, der sich beispielsweise in einem Computer des Benutzers befindet. Vorzugsweise wird der Guthabenbetrag geladen, bevor Ausdrucke von Frankierwerten erfolgen. Die Ladung des Guthabenbetrages erfolgt in einer besonders bevorzugten Ausführungsform in einem Lastschriftverfahren.

60

[0050] In Fig. 1 ist ein prinzipieller Ablauf einer erfindungsgemäßen Freimachung von Postsendungen gekennzeichnet. Das Verfahren beinhaltet mehrere Schritte, die vorzugsweise zu einem vollständigen Kreislauf ergänzt werden können. Dies ist zwar besonders zweckmäßig, jedoch nicht notwendig. Die nachfolgend dargestellte Zahl von acht Schritten ist gleichermaßen vorteilhaft, jedoch ebenfalls nicht notwendig.

65

1. Mit dem PC laden Kunden des Versandunternehmens (gegebenenfalls unter Verwendung zusätzlicher Software, zum Beispiel Microprozessor-Chipkarte) über das Internet einen Wertbetrag.
2. Über den Wertbetrag erfolgt ein Inkasso, zum Beispiel durch Abbuchung vom Konto des Kunden.
- 5 3. Aus dem Wertbetrag, der beim Kunden in einer elektronischen Börse gespeichert ist, können so lange gültige Frankierwerte in beliebiger Höhe über den eigenen Drucker ausgedruckt werden, bis das Guthaben aufgebraucht ist.
4. Der vom Kunden aufgedruckte Freimachungsvermerk enthält lesbare Angaben sowie einen maschinenlesbaren Barcode, der von der Deutschen Post zur Prüfung der Gültigkeit herangezogen wird.
- 10 5. Die freigemachte Postsendung kann über die von der Deutschen Post bereitgestellten Möglichkeiten, zum Beispiel Briefkasten und Postfilialen, eingeliefert werden.
6. Der im Freimachungsvermerk angegebene Barcode, vorzugsweise 2D-Barcode, wird im Briefzentrum über eine Anschriftenlesemaschine gelesen. Während der Produktion erfolgt eine Gültigkeitsprüfung auf logischer Plausibilitätsbasis.
- 15 7. Die im Freimachungsvermerk gelesenen Daten werden unter anderem zur Entgeltssicherung an ein Hintergrundsystem übertragen.
8. Zwischen den geladenen Abrechnungsbeträgen und den produzierten Sendungen wird zur Erkennung von Missbrauch ein Abgleich vorgenommen.

20 [0051] Vorzugsweise sind an dem Frankierungsverfahren mehrere Parteien beteiligt, wobei eine besonders zweckmäßige Aufteilung der Parteien in Fig. 2 dargestellt ist.

[0052] Die dargestellten Parteien sind ein Kunde, ein Kundensystem und ein Versandunternehmen.

25 [0053] Das Kundensystem umfasst die Hard- und Software, die vom Kunden zur PC-Frankierung eingesetzt wird. Das Kundensystem regelt in Interaktion mit dem Kunden das Laden und Speichern der Abrechnungsbeträge und den Ausdruck des Freimachungsvermerks. Einzelheiten zum Kundensystem regeln die Zulassungsvoraussetzungen.

[0054] Das Versandunternehmen übernimmt die Produktion der Sendungen und führt die erforderliche Entgeltssicherung durch.

30 [0055] Ein Wertübertragungszentrum kann auf verschiedene Weise gestaltet sein.

35 – Der Betrieb eines eigenen Wertübertragungszentrums macht in Verbindung mit der Sicherheitsarchitektur der PC-Frankierung den Einsatz symmetrischer Verschlüsselungsverfahren im Freimachungsvermerk möglich. Hierdurch wird die erforderliche Prüfzeit der Gültigkeit eines Freimachungsvermerks erheblich reduziert. Erforderlich für den Einsatz eines symmetrischen Verfahrens ist der Betrieb des Wertübertragungszentrums und der Briefzentren durch dieselbe Organisation. Eine derart beschleunigte Produktion wäre bei Verwendung asymmetrischer Sicherheitselemente im Freimachungsvermerk nicht möglich.

40 – Realisierung aller erforderlichen Sicherheitsanforderungen, unter anderem zur Vermeidung von internen und externen Manipulationen:
Anders als bei der Absenderfreistempelung erfolgt die Kommunikation über das offene und potentiell unsichere Internet. Angriffe auf die Kommunikationswege und die Internet-Server sowie interne Möglichkeiten der Manipulation erfordern höhere Sicherheitsvorkehrungen. Diese liegen in erster Linie im Interesse der Deutschen Post und deren Kunden.

45 [0056] Durch ein zentrales, durch das Versandunternehmen vorgegebenes, Management kryptographischer Schlüssel, ist eine Verbesserung der Sicherheit möglich. Die bei der Produktion im Briefzentrum relevanten Schlüssel können jederzeit durch die Deutsche Post ausgewechselt und Schlüssellängen verändert werden.

50 – Prüfungen zur Entgeltssicherung sind nach einem einheitlichen Prüfverfahren möglich und jederzeit durchführbar.
– Neue Vertragsteilnehmer und Änderungen in Verträgen können schnell allen erforderlichen Systemen des Versandunternehmens mitgeteilt werden.

55 [0057] Eine Entgeltssicherung erfolgt vorzugsweise unter Erfassung von Bestandteilen der Freimachungsvermerke.

[0058] Dazu werden Vereinbarungsdaten (Kunden-/Kundensystemdaten) aus einer zentralen Datenbank an das System übergeben, das für die Überprüfung der ordnungsgemäßen Entgeltssicherung erforderlich ist.

[0059] Den Umfang der zu speichernden Daten legt das Versandunternehmen, insbesondere der Betreiber des Postdienstes unter Beachtung von gesetzlichen Bestimmungen wie der Postdienstunternehmensdatenschutzverordnung (PDSV) fest. Grundsätzlich können danach alle Daten, die für das ordnungsgemäße Ermitteln, Abrechnen und Auswerten sowie zum Nachweis der Richtigkeit der Nachentgelte erforderlich sind, gespeichert werden. Grundsätzlich sind dies alle Sendungsinformationen ohne Empfängername und gegebenenfalls Haunummer/Postfachnummer des Empfängers.

60 [0060] Ein Hintergrundsystem überprüft, ob in dem Kundensystem enthaltene Guthabenbeträge tatsächlich in Höhe von Gebührenbeträgen verringert werden, die als Freimachungsvermerke ausgedruckt werden.

[0061] Für eine Erfassung von Vereinbarungsdaten ist vorzugsweise ein Erfassungssystem vorgesehen.

65 [0062] Vereinbarungsdaten zur PC-Frankierung mit den jeweiligen Stammdaten der Kunden und des Kundensystems (z. B. Sicherungsmodul-ID) werden über eine beispielsweise auch zu anderen Freimachungsarten einsetzbare Datenbank bereitgestellt und gepflegt. Bei Einsatz einer bestehenden Freimachungsdatenbank wird beispielsweise ein separater Teilbereich zur PC-Frankierung in der Datenbank implementiert. Die Daten werden dem Wertübertragungszentrum und Entgeltssicherungssystem im Briefzentrum bereitgestellt.

[0063] Es ist besonders zweckmäßig, dass das System Schnittstellen enthält, die einen Daten- und Informationsaustausch mit weiteren Systemen ermöglichen.

[0064] In Fig. 3 sind drei Schnittstellen dargestellt.

70 [0065] Die Schnittstellen sind mit "Freimachungsvermerk" und "Inkasso" bezeichnet. Über die Abrechnungsschnitt-

stelle werden Abrechnungsdaten zwischen dem Kundensystem und dem Versanddienstleiter ausgetauscht. Beispielsweise kann über die Abrechnungsschnittstelle ein Geldbetrag geladen werden.

[0066] Die Freimachungsschnittstelle legt fest, wie Freimachungsvermerke gestaltet werden, damit sie in Brief-, beziehungsweise Frachtzentren gelesen und geprüft werden können.

[0067] Bei der in Fig. 3 dargestellten Implementation der Schnittstellen sind die Abrechnungsschnittstellen und die Inkassoschnittstelle voneinander getrennt. Es ist jedoch gleichfalls möglich, dass die Abrechnungsschnittstelle und die Inkassoschnittstelle zusammengefasst sind, beispielsweise bei einer Abrechnung über Geldkarten, Kreditkarten oder digitales Geld, insbesondere digitale Münzen.

[0068] Die Inkassoschnittstelle legt fest, wie eine Abrechnung der über die Abrechnungsschnittstelle übermittelten Gebührenbeträge erfolgt. Die anderen Parameter des Frankierungsverfahrens hängen nicht von der gewählten Inkassoschnittstelle ab, jedoch wird durch eine effiziente Inkassoschnittstelle die Effizienz des Gesamtsystems erhöht. Bevorzugte Inkassomöglichkeiten sind Lastschriften und Rechnungen.

[0069] Nachfolgend wird dargestellt, wie durch anwendungsspezifische inhaltliche Sicherheitsanforderungen Sicherheitsziele des Frankierungsverfahrens erreicht werden.

[0070] Der Fokus dieses Konzeptes ist hierbei auf die technische Spezifikation der Sicherheitsanforderungen an das System gerichtet. Nicht sicherheitsrelevante Prozesse wie An-, Ab- und Ummelden von Kunden, die nicht über das Kundensystem erfolgen müssen, können separat festgelegt werden. Technische Prozesse zwischen dem Kundensystem und dem Kundensystemhersteller werden vorzugsweise so festgelegt, dass sie dem hier dargestellten Sicherheitsstandard entsprechen.

[0071] Durch das erfindungsgemäße Verfahren werden die nachfolgend genannten Sicherheitsziele erreicht. 20

- Phantasie- und Schmiermarken, also Freimachungsvermerke, die keine plausiblen Angaben zur Sendung enthalten oder aus anderen Gründen unleserlich sind, werden als ungültig erkannt.
- Dubletten, also exakte Kopien von gültigen Freimachungsvermerken mit plausiblen Angaben zur Sendung, können im Nachhinein erkannt werden.
- Eine Erhöhung des dem Kundensystem zur Verfügung stehenden Guthabenbetrages wird verhindert. Veränderungen des Guthabenbetrages sind auch im Nachhinein erkennbar und können vorzugsweise anhand einer Protokolliste auch im Nachhinein nachgewiesen werden.
- Unberechtigte Nutzungen werden erkannt und werden dem rechtmäßigen Nutzer im Falle einer unberechtigten Nutzung durch Dritte nicht angelastet.
- Hierzu zählt die missbräuchliche Verwertung rechtmäßig übertragener elektronischer Daten oder gültiger, rechtmäßig erzeugter Freimachungsvermerke ohne Wissen des rechtmäßigen Nutzers.
- Hierzu zählt die missbräuchliche Nutzung des Kundensystems durch Programmveränderungen.
- Hierzu zählt die unberechtigte Nutzung des Kundensystems durch fremde Softwareagenten über das Internet.
- Hierzu zählt das Ausforschen von PINs durch Angriffssoftware (trojanische Pferde).
- Hierzu zählen die Überlastungs-Angriffe (Denial-of-Service-Attacks, DoS), zum Beispiel durch Vortäuschen der Identität des Wertübertragungszentrums oder Manipulation des Ladevorgangs in der Art, dass Geld abgebucht, aber kein Guthaben angelegt wurde.

[0072] Unberechtigtes Laden von Abrechnungsbeträgen wird durch technische Vorkehrungen im Wertübertragungszentrum unmöglich gemacht. Unberechtigtes Laden von Abrechnungsbeträgen könnte z. B. erfolgen durch: 40

- Vortäuschen der Identität des Post-Wertübertragungszentrums zur Erhöhung der eigenen Börse im Kundensystem durch den Kunden.
- Vortäuschen eines zertifizierten Kundensystems durch ein manipuliertes oder erfundenes Kundensystem derart, dass der Täter Kenntnis von sicherheitskritischen Geheimnissen des Sicherungsmoduls erlangt und daraufhin unbemerkt Fälschungen erstellen kann.
- Mitschneiden der ordnungsgemäßen Kommunikation zwischen einem Kundensystem und dem Wertübertragungszentrum und Wiederholung dieser Kommunikation in missbräuchlicher Absicht (Replay-Attacke).
- Manipulation der zwischen Kundensystem und Wertübertragungszentrum stattfindenden Kommunikation in Echtzeit (ein- und ausgehende Datenströme im Kundensystem) in der Weise, dass das Kundensystem von einem höheren geladenen Wertbetrag als das Wertübertragungszentrum ausgeht.
- Missbrauch von Kundenidentifikationsnummern in der Weise, dass Dritte auf Kosten eines Kunden Wertbeträge laden.
- Unvollständige Stornoabwicklung.

[0073] Die ersten beiden dieser Sicherheitsprobleme werden im Wesentlichen durch das Systemkonzept und die durch Maßnahmen im Gesamtsystem gelöst, die drei letzten werden vorzugsweise durch die Implementation von Soft- und Hardware des Sicherungsmoduls gelöst.

[0074] Bevorzugte Ausgestaltungen einer die Sicherheitsstandards erhöhenden Hardware sind nachfolgend dargestellt: 60 Grundlegende Eigenschaften der Hardware

1. Alle Verschlüsselungen, Entschlüsselungen, Umschlüsselungen, Signaturberechnungen und kryptographischen Prüfungsprozeduren werden in gegen unberechtigte Zugriffe besonders geschützten Bereichen eines kryptographischen Sicherungsmoduls im Kundensystem durchgeführt. Die zugehörigen Schlüssel sind ebenfalls in solchen Sicherheitsbereichen abgelegt.
2. Sicherheitsrelevante Daten und Abläufe (zum Beispiel Schlüssel, Programme) werden gegen unberechtigte Veränderungen und geheime Daten (zum Beispiel Schlüssel, PINs) gegen unberechtigtes Auslesen geschützt. Dies wird

vorzugsweise durch folgende Maßnahmen gewährleistet:

- Bauart des Sicherungsmoduls, eventuell im Zusammenwirken mit Sicherheitsmechanismen der Software des Sicherungsmoduls,
- Laden von Programmen in Sicherungsmodule nur bei der Herstellung oder kryptographischer Absicherung des Ladevorgangs,
- kryptographische Absicherung des Ladens von sicherheitsrelevanten Daten, insbesondere von kryptographischen Schlüsseln.
- Auch vor dem Auslesen mittels Angriffen, die die Zerstörung des Moduls in Kauf nehmen, müssen geheime Daten in Sicherungsmodulen geschützt sein.

10 a. Der Schutz von Daten und Programmen gegen Veränderung, beziehungsweise Auslesen in dem Sicherungsmodul muss so hoch sein, dass während der Lebensdauer des Moduls Angriffe mit vertretbarem Aufwand nicht möglich sind, wobei der für einen erfolgreichen Angriff nötige Aufwand gegen den hieraus zu ziehenden Nutzen abzuwegen ist.

15 b. Unerwünschte Funktionen dürfen durch ein Sicherungsmodul nicht ausführbar sein.

15 [0075] Unerwünschte Nebenfunktionen und zusätzliche Datenkanäle, insbesondere Schnittstellen, die ungewollt Informationen weitergeben (Side Channels), werden verhindert.

[0076] Durch die Konstruktion des Sicherungsmoduls wird sichergestellt, dass ein Angreifer Informationen über geheimzuhaltende Daten und Schlüssel nicht über Schnittstellen auslesen kann, die für andere Zwecke gedacht sind.

20 [0077] Das Vorliegen solcher Kanäle von Side Channels wird durch entsprechende Tests überprüft. Typische Möglichkeiten, die überprüft werden, sind:

1. Single Power Attack (SPA) und Differential Power Attack (DPA), die versuchen, aus Änderungen des Stromverbrauchs während kryptographischer Berechnungen auf geheime Daten zu schließen.

25 2. Timing Attacks, die versuchen, aus der Dauer kryptographischer Berechnungen auf geheime Daten zu schließen.

[0078] Bevorzugte Eigenschaften der Datenverarbeitung sind nachfolgend dargestellt:

Ablaufkontrolle

30 [0079] Es ist besonders zweckmäßig, dass eine Ablaufkontrolle durchgeführt wird. Diese kann beispielsweise durch eine Zustandsmaschine, beispielsweise entsprechend dem Standard FIPS PUB 140-1, erfolgen. Dadurch wird sichergestellt, dass die Abläufe der spezifizierten Transaktionen und die hierbei verwendeten sicherheitsrelevanten Daten des Systems nicht manipuliert werden können.

35 [0080] Die beteiligten Instanzen, insbesondere der Benutzer, dürfen durch ein Sicherungsmodul über die Abläufe der Transaktionen nicht getäuscht werden.

[0081] Wenn beispielsweise der Vorgang des Ladens eines Wertbetrages in der Form mehrerer Teilvorgänge mit einzelnen Aufrufen des Sicherungsmoduls realisiert ist, muss die Ablaufkontrolle sicherstellen, dass diese Teilvorgänge nur in der zulässigen Reihenfolge ausgeführt werden.

40 [0082] Die Zustandsdaten, die für die Ablaufkontrolle verwendet werden, sind sicherheitsrelevant und werden daher vorzugsweise in einem gegen Manipulation gesicherten Bereich des Sicherungsmoduls gespeichert.

Nachrichtenintegrität

45 1. Alle sicherheitsrelevanten Informationen in den Nachrichten werden vor und nach der Übertragung in den Komponenten des Systems mit geeigneten Verfahren gegen unberechtigte Veränderung geschützt.

2. Veränderungen an sicherheitsrelevanten Informationen während der Übertragung zwischen Komponenten des chipkartengestützten Zahlungssystems werden erkannt. Entsprechende Reaktionen auf Integritätsverletzungen müssen erfolgen.

50 3. Das unautorisierte Einspielen von Nachrichten wird erkannt. Entsprechende Reaktionen müssen auch auf wieder eingespilte Nachrichten erfolgen.

55 [0083] Dass unbefugte Veränderungen und das Wiedereinspielen von Nachrichten erkannt werden können, wird für die Standardnachrichten des Systems durch die Festlegungen des Systemkonzepts sichergestellt. Die Software des Sicherungsmoduls hat sicherzustellen, dass die Erkennung tatsächlich erfolgt und entsprechend reagiert wird. Für sicherheitsrelevante herstellerspezifische Nachrichten (etwa im Rahmen der Personalisierung der Wartung des Sicherungsmoduls) werden entsprechende geeignete Mechanismen festgelegt und angewendet.

60 [0084] Die für die Sicherung der Nachrichtenintegrität relevanten Informationen werden vorzugsweise in einem gegen Manipulation gesicherten Bereich des Sicherungsmoduls gespeichert. Solche Informationen sind insbesondere Identifikations- und Authentizitätsmerkmale, Sequenzzähler oder Gebührenbeträge.

Geheimhaltung von PINs und kryptographischen Schlüsseln

65 1. Obwohl die PIN außerhalb von gesicherten Bereichen nicht im Klartext übertragen werden sollte, wird vorzugsweise die Klartext-Übertragung bei der PC-Frankierung aus Gründen der Benutzerfreundlichkeit des Gesamtsystems und der Verwendung bestehender, ungesicherter Hardwarekomponenten im Kundensystem (Tastatur, Monitor) toleriert. Jedoch sind die lokalen Systemkomponenten, in denen die PINs im Klartext bearbeitet oder gespeichert werden, auf ein Minimum zu reduzieren. Eine ungesicherte Übertragung der PINs darf nicht erfolgen.

2. Kryptographische Schlüssel dürfen auf elektronischen Übertragungswegen in ungesicherter Umgebung nie im Klartext übertragen werden. Werden sie in Systemkomponenten benutzt oder gespeichert, so müssen sie gegen unautorisiertes Auslesen und Verändern geschützt sein.
3. Keine Systemkomponente darf eine Möglichkeit zur Bestimmung einer PIN aufgrund einer erschöpfenden Suche bieten.

5

Protokollierung

1. Innerhalb des Kundensystems werden alle Daten protokolliert, die für die Rekonstruktion der betreffenden Abläufe benötigt werden. Ferner werden auch Fehlerfälle protokolliert, die einen Manipulationsverdacht nahelegen.
2. Gespeicherte Protokolldaten müssen gegen unberechtigte Veränderungen geschützt sein und authentisch an eine auswertende Instanz übertragen werden können.

10

Verarbeitung anderer Anwendungen

[0085] Werden in Sicherungsmodulen gleichzeitig andere Anwendungen verarbeitet, so darf dadurch die Sicherheit des PC-Frankierungssystems nicht beeinflusst werden.

15

[0086] Durch folgende Maßnahmen kann die Datensicherheit weiter erhöht werden:

- Löschen geheimer Daten aus temporären Speichern
- Sichere Implementation von herstellerspezifischen Funktionen (z. B. im Rahmen der Personalisierung); etwa Verwendung von Triple-DES oder einem sicheren symmetrischen Verfahren für Verschlüsselung von geheimen Personalisierungsdaten, Einbringung von Klartextschlüsseln in Form von geteilten Geheimnissen (z. B. Schlüsselhälften) nach dem Vier-Augen-Prinzip
- Es dürfen keine unsicheren Zusatzfunktionen existieren (etwa Verschlüsseln oder Entschlüsseln oder Signieren von frei wählbaren Daten mit Schlüsseln des Systems); es darf keine Funktionsvertauschung von Schlüsseln möglich sein.

20

25

Weitere Aspekte

30

- Ausser den in den Kundensystemen eingesetzten Sicherungsmodulen sind auch weitere Sicherungsmodule zu untersuchen: Insbesondere sind die Sicherungsmodule der verschiedenen Zertifizierungsstellen (CAs) bei den Herstellern von Sicherungsmodulen zu untersuchen.
- Auch der PC-seitige Anteil der Kundensoftware ist hinsichtlich seiner sicherheitsrelevanten Aufgaben (z. B. PIN-Eingabe) zu untersuchen.
- Es ist vom Hersteller eines Kundensystems ein Verfahren vorzusehen, das die gesicherte Übermittlung der PIN von Sicherungsmodulen an die Benutzer garantiert (Beispielsweise PIN-Brief-Versendung). Ein solches Konzept ist auf Sicherheit und Einhaltung zu überprüfen. Sicherheit der Herstellerumgebung, insbesondere Schlüsseleinbringung etc.; Sicherheitsbeauftragte, allgemeiner: Zulassung der organisatorischen Sicherheitsmaßnahmen von Herstellern nach festgelegtem Verfahren. Im Einzelnen:

35

40

Schlüsselmanagement

1. Zur Verteilung, Verwaltung und eventuell zum turnusmässigen Wechsel und zum Ersetzen von Schlüsseln sind Regelungen zu treffen.
2. Schlüssel, für die der Verdacht auf Kompromittierung besteht, dürfen im gesamten System nicht mehr verwendet werden.

45

[0087] Bevorzugte Maßnahmen bei der Herstellung und Personalisierung von Sicherungsmodulen sind:

50

1. Die Herstellung und Personalisierung (Ersteinbringung geheimer Schlüssel, eventuell benutzerspezifischer Daten) von Sicherungsmodulen muss in einer Produktionsumgebung stattfinden, die verhindert, dass
 - Schlüssel bei der Personalisierung kompromittiert werden,
 - der Personalisierungsvorgang missbräuchlich oder unberechtigt durchgeführt wird,
 - unauthorizede Software oder Daten eingebracht werden können,
 - Sicherungsmodule entwendet werden.
2. Es muss sichergestellt sein, dass in das System keine unauthorizeden Komponenten eingebracht werden können, die sicherheitsrelevante Funktionen ausführen.
3. Der Lebensweg aller Sicherungsmodule muss kontinuierlich aufgezeichnet werden.

55

60

Erläuterung

[0088] Die Aufzeichnung des Lebenswegs eines Sicherungsmoduls umfasst:

65

- Herstellungs- und Personalisierungsdaten,
- räumlichen/zeitlichen Verbleib,

- Reparatur und Wartung,
- Ausserbetriebnahme,
- Verlust bzw. Diebstahl von das Sicherungsmodul enthaltenden Datenspeichern wie Dateien, Dongles, Krypto, Server oder Chipkarten

5 - Herstellungs- und Personalisierungsdaten,

- Einbringen neuer Anwendungen,
- Änderung von Anwendungen,
- Änderung von Schlüsseln,
- Ausserbetriebnahme,

10 - Verlust bzw. Diebstahl.

Sicherheitsarchitektur

15 [0089] Für die PC-Frankierung wird eine grundsätzliche Sicherheitsarchitektur vorgesehen, die die Vorteile verschiedener, bestehender Ansätze verbindet und mit einfachen Mitteln ein höheres Maß an Sicherheit bietet.

[0090] Die Sicherheitsarchitektur umfasst vorzugsweise im Wesentlichen drei Einheiten, die in einer bevorzugten Anordnung in Fig. 4 dargestellt sind:

20 - Ein Wertübertragungszentrum, in dem die Identität des Kunden und seines Kundensystems bekannt ist.

- Ein Sicherungsmodul, das die nicht durch den Kunden manipulierbare Hard-/Software die Sicherheit im Kundensystem gewährleistet (z. B. Dongle oder Chipkarte bei Offline-Lösungen bzw. gleichwertige Server bei Online-Lösungen).

25 - Ein Briefzentrum, in dem die Gültigkeit der Freimachungsvermerke geprüft, beziehungsweise Manipulationen am Wertbetrag sowie am Freimachungsvermerk erkannt werden.

[0091] Die einzelnen Prozessschritte, die im Wertübertragungszentrum, Kundensystem und Briefzentrum erfolgen, sollen im Folgenden in Form einer Prinzipskizze dargestellt werden. Der genaue technische Kommunikationsprozess weicht hingegen von dieser prinzipiellen Darstellung ab (z. B. mehrere Kommunikationsschritte zur Erlangung einer hier dargestellten Übertragung). Insbesondere wird in dieser Darstellung eine vertrauliche und integre Kommunikation zwischen identifizierten und authentisierten Kommunikationspartnern vorausgesetzt.

Kundensystem

35 [0092] 1. Innerhalb des Sicherungsmoduls wird eine Zufallszahl erzeugt und zwischengespeichert, die dem Kunden nicht zur Kenntnis gelangt.

[0093] 2. Innerhalb des Sicherungsmoduls wird die Zufallszahl zusammen mit einer eindeutigen Identifikationsnummer (Sicherungsmodul-ID) des Kundensystems, beziehungsweise des Sicherungsmoduls, derart kombiniert und verschlüsselt, dass nur das Wertübertragungszentrum in der Lage ist, eine Entschlüsselung durchzuführen.

40 [0094] In einer besonders bevorzugten Ausführungsform wird die Zufallszahl zusammen mit einem zuvor vom Wertübertragungszentrum ausgegebenen Sitzungsschlüssel und den Nutzdaten der Kommunikation (Beantragung der Einrichtung eines Abrechnungsbetrages) mit dem öffentlichen Schlüssel des Wertübertragungszentrums verschlüsselt und mit dem privaten Schlüssel des Sicherungsmoduls digital signiert. Hierdurch wird vermieden, dass die Anfrage bei jedem Laden eines Abrechnungsbetrages dieselbe Gestalt hat und zum missbräuchlichen Laden von Abrechnungsbeträgen herangezogen werden kann (Replay-Attack).

45 [0095] 3. Die kryptographisch behandelten Informationen aus dem Kundensystem werden an das Wertübertragungszentrum im Rahmen des Ladens eines Abrechnungsbetrages übertragen. Weder der Kunde noch Dritte können diese Informationen entschlüsseln.

[0096] In der Praxis wird die asymmetrische Verschlüsselung mit dem öffentlichen Schlüssel des Kommunikationspartners (Wertübertragungszentrum, beziehungsweise Sicherungsmodul) angewandt.

50 [0097] Bei der Möglichkeit eines vorhergehenden Austausches von Schlüsseln kommt eine symmetrische Verschlüsselung gleichfalls in Betracht.

Wertübertragungszentrum

55 [0098] 4. Im Wertübertragungszentrum wird unter anderem die Zufallszahl, die der Identifikationsnummer des Sicherungsmoduls (Sicherungsmodul-ID) zugeordnet werden kann, entschlüsselt.

[0099] 5. Durch Anfrage in der Datenbank-Freimachung wird die Sicherungsmodul-ID ein Kunde der Deutschen Post zugeordnet.

60 [0100] 6. Im Wertübertragungszentrum wird eine Ladevorgangsidentifikationsnummer gebildet, die Teile der Sicherungsmodul-ID, die Höhe eines Abrechnungsbetrages etc. beinhaltet. Die entschlüsselte Zufallszahl wird zusammen mit der Ladevorgangsidentifikationsnummer derart verschlüsselt, dass nur das Briefzentrum in der Lage ist, eine Entschlüsselung durchzuführen. Der Kunde ist hingegen nicht in der Lage, diese Informationen zu entschlüsseln. (Die Ladevorgangsidentifikationsnummer wird zusätzlich in einer vom Kundensystem entschlüsselbaren Form verschlüsselt). In der Praxis erfolgt die Verschlüsselung mit einem symmetrischen Schlüssel nach TDES, der ausschließlich im Wertübertragungszentrum sowie in den Briefzentren vorhanden ist. Die Verwendung der symmetrischen Verschlüsselung an dieser Stelle ist begründet durch die Forderung schneller Entschlüsselungsverfahren durch die Produktion.

65 [0101] 7. Die verschlüsselte Zufallszahl und die verschlüsselte Ladevorgangsidentifikationsnummer werden an das

Kundensystem übertragen. Weder der Kunde noch Dritte können diese Informationen entschlüsseln. Durch die alleinige Verwaltung des posteigenen, vorzugsweise symmetrischen Schlüssels im Wertübertragungszentrum und in den Briefzentren kann der Schlüssel jederzeit ausgetauscht und Schlüssellängen können bei Bedarf geändert werden. Hierdurch wird auf einfache Weise eine hohe Manipulationssicherheit gewährleistet. In der Praxis wird die Ladevorgangsidentifikationsnummer dem Kunden zusätzlich in nicht verschlüsselter Form zur Verfügung gestellt.

5

Kundensystem

[0102] 8. Der Kunde erfasst im Rahmen der Erstellung eines Freimachungsvermerks die sendungsspezifischen Informationen oder Sendungsdaten (z. B. Porto, Sendungsart etc.), die in das Sicherungsmodul übertragen werden.

10

[0103] 9. Innerhalb des Sicherungsmoduls wird ein Hash-Wert unter anderem aus folgenden Informationen gebildet

- Auszügen aus den Sendungsdaten (z. B. Porto, Sendungsart, Datum, PLZ etc.),
- der zwischengespeicherten Zufallszahl (die im Rahmen des Ladens eines Abrechnungsbetrages erzeugt wurde)
- und gegebenenfalls der Ladevorgangsidentifikationsnummer.

15

[0104] 10. In den Freimachungsvermerk werden unter anderem folgende Daten übernommen:

- Auszüge aus den Sendungsdaten im Klartext (z. B. Porto, Sendungsart, Datum, PLZ etc.),
- die verschlüsselte Zufallszahl und die verschlüsselte Ladevorgangsidentifikationsnummer aus dem Wertübertragungszentrum und
- der innerhalb des Sicherungsmoduls gebildete Hash-Wert aus Sendungsdaten, Zufallszahl und Ladevorgangsidentifikationsnummer.

20

Briefzentrum

25

[0105] 11. Im Briefzentrum werden zunächst die Sendungsdaten geprüft. Stimmen die in den Freimachungsvermerk übernommenen Sendungsdaten nicht mit der Sendung überein, so liegen entweder eine Falschfrankierung, eine Phantasie- oder eine Schmiermarke vor. Die Sendung ist der Entgeltsicherung zuzuführen.

30

[0106] 12. Im Briefzentrum werden die Zufallszahl und die Ladevorgangsidentifikationsnummer, die im Rahmen des Abrechnungsbetrages an das Kundensystem übergeben wurden, entschlüsselt. Hierzu ist im Briefzentrum nur ein einziger (symmetrischer) Schlüssel erforderlich. Bei Verwendung von individuellen Schlüsseln wäre jedoch statt dessen eine Vielzahl von Schlüsseln einzusetzen.

[0107] 13. Im Briefzentrum wird nach demselben Verfahren wie in dem Sicherungsmodul ein Hash-Wert aus folgenden Informationen gebildet:

35

- Auszügen aus den Sendungsdaten,
- der entschlüsselten Zufallszahl
- der entschlüsselten Ladevorgangsidentifikationsnummer.

40

[0108] 14. Im Briefzentrum werden der selbstgebildete und der übertragene Hash-Wert verglichen. Stimmen beide überein, so wurde der übertragene Hash-Wert mit derselben Zufallszahl gebildet, die auch dem Wertübertragungszentrum im Rahmen des Ladens des Abrechnungsbetrages übermittelt wurde. Demnach handelt es sich sowohl um einen echten, gültigen Abrechnungsbetrag als auch um Sendungsdaten, die dem Sicherungsmodul bekanntgegeben wurden (Gültigkeitsprüfung). Vom Aufwand her entsprechen die Entschlüsselung, die Bildung eines Hash-Wertes und der Vergleich von zwei Hash-Werten theoretisch dem einer Signaturprüfung. Aufgrund der symmetrischen Entschlüsselung entsteht jedoch gegenüber der Signaturprüfung ein zeitlicher Vorteil.

45

[0109] 15. Über eine Gegenprüfung im Hintergrundsystem können im Nachhinein Abweichungen zwischen geladenen Abrechnungsbeträgen und Frankierbeträgen ermittelt werden (Überprüfung hinsichtlich Sendungsdoubletten, Saldenbildung im Hintergrundsystem).

50

[0110] Die dargestellte grundsätzliche Sicherheitsarchitektur umfasst nicht die separat abgesicherte Verwaltung der Abrechnungsbeträge (Börsenfunktion), die Absicherung der Kommunikation zwischen Kundensystem und dem Wertübertragungszentrum, die gegenseitige Identifizierung von Kundensystem und Wertübertragungszentrum und die Initialisierung zur sicheren Betriebsaufnahme eines neuen Kundensystems.

55

Angriffe auf die Sicherheitsarchitektur

[0111] Die beschriebene Sicherheitsarchitektur ist sicher gegenüber Angriffen durch Folgendes:

60

- Dritte können die im Internet mitgeschnittene (kopierte) erfolgreiche Kommunikation zwischen einem Kundensystem und dem Wertübertragungszentrum nicht zu betrügerischen Zwecken nutzen (Replay-Attacke).
- Dritte oder Kunden können gegenüber dem Wertübertragungszentrum nicht die Verwendung eines ordnungsgemäßen Kundensystems durch ein manipuliertes Kundensystem vortäuschen. Spiegelt ein Dritter oder ein Kunde die Übertragung einer Zufallszahl und einer Safe-Box-ID vor, die nicht innerhalb eines Sicherungsmoduls erzeugt wurden, sondern ihm bekannt sind, so scheitert das Laden der Abrechnungsbeträge entweder an der separat durchgeführten Identifikation des rechtmäßigen Kunden durch Benutzername und Kennwort oder an der Kenntnis des privaten Schlüssels des Sicherungsmoduls, der dem Kunden unter keinen Umständen bekannt sein darf. (Deshalb ist

65

der Initialisierungsprozess zur Schlüsselerzeugung in dem Sicherungsmodul und die Zertifizierung des öffentlichen Schlüssels durch den Kundensystemanbieter geeignet durchzuführen.)

- Dritte oder Kunden können nicht mit einem vorgetäuschten Wertübertragungszentrum gültige Abrechnungsbezüge in ein Kundensystem laden. Spiegelt ein Dritter oder ein Kunde die Funktionalität des Wertübertragungszentrums vor, so gelingt es diesem vorgespiegelten Wertübertragungszentrum nicht, eine verschlüsselte Ladevorgangsidentifikationsnummer zu erzeugen, die im Briefzentrum ordnungsgemäß entschlüsselt werden kann. Zudem kann das Zertifikat des öffentlichen Schlüssels des Wertübertragungszentrums nicht gefälscht werden.
- Kunden können nicht unter Umgehung des Wertübertragungszentrums einen Freimachungsvermerk erstellen, dessen Ladevorgangsidentifikationsnummer derart verschlüsselt ist, dass sie im Briefzentrum als gültig entschlüsselt werden könnte.

[0112] Zur Erhöhung der Datensicherheit, insbesondere beim Suchen, ist eine erschöpfende Anzahl von Zufallszahlen zur Hash-Wert-Bildung heranzuziehen.

15 – Die Länge der Zufallszahl ist daher möglichst gross und beträgt vorzugsweise mindestens 16 byte (128 bit).

[0113] Die eingesetzte Sicherheitsarchitektur ist durch die Möglichkeit, kundenspezifische Schlüssel einzusetzen, ohne dass es notwendig ist, in zur Entschlüsselung bestimmten Stellen, insbesondere Briefzentren, Schlüssel bereit zu halten, den bekannten Verfahren überlegen. Diese vorteilhafte Ausgestaltung ist ein wesentlicher Unterschied zu den bekannten 20 Systemen nach dem Information-Based Indicia Program (IBIP).

[0114] Falls keine Signaturprüfung wie im Modell IBIP erfolgt, würde keine wesentlich höhere Sicherheit als bei der Absenderfreistempelung erzielt. Wird zudem die Tatsache bekannt, dass die digitalen Signaturen nicht geprüft werden, könnte dies zu einem Anstieg des Missbrauchs führen. Werden nämlich in missbräuchlicher Absicht alle Angaben, die zur Plausibilitätsprüfung herangezogen werden, gefälscht, ohne jedoch eine gültige Signatur anzufügen, so kann dieser 25 Missbrauch auch bei erheblichem Umfang außerhalb von Stichproben nicht erkannt werden.

Vorteile der Sicherheitsarchitektur

[0115] Folgende Merkmale zeichnen die beschriebene Sicherheitsarchitektur gegenüber dem IBIP-Modell der USA 30 aus:

- Die eigentliche Sicherheit wird in den Systemen der Deutschen Post (Wertübertragungszentrum, Briefzentrum, Entgeltsicherungssystem) gewährleistet und ist damit vollständig im Einflussbereich der Deutschen Post.
- Es werden im Freimachungsvermerk keine Signaturen, sondern technisch gleichwertige und ebenso sichere (symmetrisch) verschlüsselte Daten und Hash-Werte angewandt. Hierzu wird im einfachsten Falle nur ein symmetrischer Schlüssel verwendet, der alleine im Einflussbereich der Deutschen Post liegt und somit leicht austauschbar ist.
- Im Briefzentrum ist eine Überprüfung aller Freimachungsmerkmale (nicht bloß stichprobenweise) möglich.
- Das Sicherheitskonzept basiert auf einem einfachen, in sich geschlossenen Prüfkreislauf, der in Einklang mit einem hierauf angepaßten Hintergrundsystem steht.
- Das System macht selbst ansonsten kaum feststellbare Dubletten erkennbar.
- Ungültige Phantasiemarken sind mit diesem Verfahren mit hoher Genauigkeit erkennbar.
- Neben der Plausibilitätsprüfung kann bei allen Freimachungsvermerken eine Überprüfung der Ladevorgangsidentifikationsnummer in Echtzeit erfolgen.

45

Sendungsarten

[0116] Mit der PC-Frankierung können alle Produkte des Versendungsdienstleisters wie beispielsweise "Brief national" (einschließlich Zusatzleistungen) und "Direkt Marketing national" gemäß einer vorhergehenden Festlegung durch 50 den Versendungsdienstleister freigemacht werden.

[0117] Ein Einsatz für andere Versandformen wie Paket- und Expresssendungen ist gleichermaßen möglich.

[0118] Der Gebührenbetrag, der maximal über das Wertübertragungszentrum geladen werden kann, wird auf einen geeigneten Betrag festgelegt. Der Betrag kann je nach Anforderung des Kunden und dem Sicherheitsbedürfnis des Postdienstleisters gewählt werden. Während für einen Einsatz im Privatkundenbereich ein Gebührenbetrag von maximal mehreren hundert DM besonders zweckmäßig ist, werden für Einsätze bei Grosskunden wesentlich höhere Gebührenbezüge vorgesehen. Ein Betrag in der Größenordnung von etwa DM 500,- eignet sich sowohl für anspruchsvolle Privathaushalte als auch für Freiberufler und kleinere Unternehmen. Der in der Börse gespeicherte Wert sollte vorzugsweise den doppelten Wertbetrag systemtechnisch nicht überschreiten.

60

Falschfrankierte Sendungen

[0119] Falschfrankierte und nicht zur Beförderung geeignete, bereits bedruckte Schreiben, Umschläge etc. mit einem gültigen Freimachungsvermerk werden dem Kunden gutgeschrieben.

[0120] Durch geeignete Maßnahmen, beispielsweise durch eine Stempelung von in dem Briefzentrum eingehenden 65 Sendungen, ist es möglich festzustellen, ob eine Sendung bereits befördert wurde. Hierdurch wird verhindert, dass Kunden bereits beförderte Sendungen vom Empfänger zurück erhalten und diese zur Gutschrift bei dem Postdienstbetreiber, beispielsweise der Deutschen Post AG, einreichen.

[0121] Die Rücksendung an eine zentrale Stelle des Versendungsdienstleisters, beispielsweise der Deutschen Post, ermöglicht ein hohes Maß an Entgeltsicherung durch Abgleich der Daten mit Abrechnungsbeträgen und die Kenntnis über die häufigsten Zusendungsgründe. Hierdurch besteht gegebenenfalls die Möglichkeit der Nachsteuerung durch Änderung der Einführungsvoraussetzungen mit dem Ziel der Reduzierung der Rücksendekontrakte. 5

Gültigkeit von Freimachungswerten

[0122] Vom Kunden gekaufte Abrechnungswerte sind aus Gründen der Entgeltsicherung beispielsweise nur 3 Monate gültig. Ein entsprechender Hinweis ist in der Vereinbarung mit dem Kunden aufzunehmen. Können Frankierwerte nicht innerhalb von 3 Monaten aufgebraucht werden, muss vom Kundensystem die Kontaktierung des Wertübertragungszentrums zu einer erneuten Herstellung von Freimachungsvermerken aufgenommen werden. Bei dieser Kontaktierung wird, wie beim ordentlichen Laden von Abrechnungsbeträgen, der Restbetrag eines alten Abrechnungsbetrages einem neu ausgegebenen Abrechnungsbetrag zugeschlagen und unter einer neuen Ladevorgangsidentifikationsnummer dem Kunden zur Verfügung gestellt wird. 10

Besondere betriebliche Behandlung

[0123] Grundsätzlich können die Freimachungsvermerke eine beliebige Form aufweisen, in der die in ihnen enthaltenen Informationen wiedergegeben werden können. Es ist jedoch zweckmäßig, die Freimachungsvermerke so zu gestalten, dass sie wenigstens bereichsweise die Form von Barcodes aufweisen. Bei der dargestellten Lösung des 2D-Barcodes und der daraus resultierenden Entgeltsicherung sind folgende Besonderheiten in der Produktion zu berücksichtigen: 20

PC-frankierte Sendungen können über alle Einlieferungsmöglichkeiten, auch über Briefkasten, eingeliefert werden. [0124] Durch die Festlegung von Zulassungsvoraussetzungen für Hersteller von für die Schnittstellen relevanten Bestandteilen des Frankierungssystems, insbesondere für Hersteller und/oder Betreiber von Kundensystemen, wird die Einhaltung der dargestellten Sicherheitsmaßnahmen weiter erhöht. 25

Übergeordnete Normen, Standards und Vorgaben

International Postage Meter Approval Requirements (IPMAR)

[0125] Vorzugsweise finden die Vorschriften der aktuellsten Fassung des Dokuments International Postage Meter Approval Requirements (IPMAR), UPU S-30, ebenso Anwendung wie alle Normen und Standards, auf die in diesem Dokument verwiesen wird. Die Einhaltung aller dort genannten "Requirements" ist, soweit möglich, für das Kundensystem sinnvoll. 30

Digital Postage Marks: Applications, Security & Design

[0126] Grundsätzlich finden die Vorschriften der aktuellen Fassung des Dokuments Digital Postage Marks: Applications, Security & Design (UPU: Technical Standards Manual) ebenso Anwendung wie alle Normen und Standards, auf die in diesem Dokument verwiesen wird. Die Einhaltung des "normativen" Inhalts sowie die weitestgehende Beachtung des "informativen" Inhalts dieses Dokuments ist, soweit möglich, für das Kundensystem sinnvoll. 40

[0127] Vorzugsweise finden Regelungen und Bestimmungen des Versendungsdienstleistungsunternehmens gleichfalls Anwendung.

[0128] Durch eine Zulassung lediglich solcher Systeme, die alle gesetzlichen Bestimmungen ebenso erfüllen wie alle Normen und Standards des Versendungsdienstleisters, werden Datensicherheit und Zuverlässigkeit des Systems ebenso gewährleistet wie seine Benutzerfreundlichkeit. 45

Weitere Gesetze, Verordnungen, Richtlinien, Vorschriften Normen und Standards

[0129] Grundsätzlich finden alle Gesetze, Verordnungen, Richtlinien, Vorschriften, Normen und Standards der jeweils gültigen Fassung Anwendung, die zur Entwicklung und zum Betrieb eines technischen Kundensystems in der konkreten Ausprägung zu beachten sind. 50

Systemtechnische Interoperabilität

[0130] Die systemtechnische Interoperabilität bezieht sich auf die Funktionsfähigkeit der Schnittstellen des Kundensystems, beziehungsweise auf die Einhaltung der in den Schnittstellenbeschreibungen spezifizierten Vorgaben. 55

Schnittstelle Abrechnungsbetrag

Kommunikationsweg, Protokolle

[0131] Die Kommunikation über die Schnittstelle Abrechnungsbetrag erfolgt vorzugsweise über das öffentliche Internet auf der Basis der Protokolle TCP/IP und HTTP. Der Datenaustausch kann optional per HTTP über SSL verschlüsselt werden (https). Hier dargestellt ist der Soll-Prozess einer erforderlichen Übertragung. 60

[0132] Der Datenaustausch erfolgt vorzugsweise, sofern möglich, über HTML- und XML-kodierte Dateien. Die textlichen und graphischen Inhalte der HTML-Seiten sind im Kundensystem darzustellen.

[0133] Es erscheint empfehlenswert, bei den Kommunikationsseiten auf eine bewährte HTML-Version zurückzugreifen. 65

fen und auf die Verwendung von Frames, eingebetteten Objekten (Applets, Activex etc.) und ggf. animierten GIFs zu verzichten.

5 Anmeldung zum Laden eines Abrechnungsbetrages (erste Übertragung von dem Sicherungsmodul zum Wertübertragungszentrum)

[0134] Im Rahmen der ersten Übertragung von dem Sicherungsmodul zum Wertübertragungszentrum werden das Zertifikat des Sicherungsmoduls sowie ein Aktionsindikator A unverschlüsselt und unsigniert übertragen.

10 Rückmeldung zur Anmeldung (erste Antwort vom Wertübertragungszentrum zum Sicherungsmodul)

[0135] Die Rückmeldung des Wertübertragungszentrums enthält das eigene Zertifikat des Wertübertragungszentrums, einen verschlüsselten Sitzungsschlüssel und die digitale Signatur des verschlüsselten Sitzungsschlüssels.

15 Zweite Übertragung von dem Sicherungsmodul zum Wertübertragungszentrum

[0136] Im Rahmen dieser Übertragung sendet das Sicherungsmodul den neu verschlüsselten Sitzungsschlüssel, die verschlüsselte Zufallszahl und den verschlüsselten Datensatz mit Nutzdaten (Höhe eines vorab geladenen Abrechnungsbetrages, Restwert des aktuellen Abrechnungsbetrages, aufsteigendes Register aller Abrechnungsbeträge, letzte Ladevorgangsidentifikationsnummer) an das Wertübertragungszentrum (alles asymmetrisch mit dem öffentlichen Schlüssel des Wertübertragungszentrums verschlüsselt). Gleichzeitig sendet das Sicherungsmodul die digitale Signatur dieser verschlüsselten Daten an das Wertübertragungszentrum. Gleichzeitig kann das Kundensystem weitere, nicht verschlüsselte und nicht signierte Nutzungsprotokolle oder Nutzungsprofile an das Wertübertragungszentrum senden.

[0137] Es ist zweckmäßig, dass die Nutzungsdaten in ein Nutzungsprotokoll eingetragen werden und dass das Nutzungsprotokoll und/oder die darin vermerkten Einträge digital signiert werden.

Zweite Antwort vom Wertübertragungszentrum zu dem Sicherungsmodul

[0138] Das Wertübertragungszentrum übermittelt die symmetrisch verschlüsselte Zufallszahl und die symmetrisch verschlüsselte Ladevorgangsidentifikationsnummer an das Sicherungsmodul. Außerdem übermittelt das Wertübertragungszentrum die mit dem öffentlichen Schlüssel des Sicherungsmoduls Ladevorgangsidentifikationsnummer, Login-Informationen für das Sicherungsmodul sowie einen neuen Sitzungsschlüssel an das Sicherungsmodul. Die gesamten übertragenen Daten werden zudem digital signiert.

35 Dritte Übertragung von dem Sicherungsmodul zum Wertübertragungszentrum

[0139] Im Rahmen der dritten Übertragung werden von dem Sicherungsmodul der neue Sitzungsschlüssel, die neue Ladevorgangsidentifikationsnummer zusammen mit Nutzdaten zur Bestätigung der erfolgreichen Kommunikation alleamt in verschlüsselter und digital signierter Form an das Wertübertragungszentrum übertragen.

40 Dritte Antwort vom Wertübertragungszentrum an das Sicherungsmodul

[0140] Bei der dritten Antwort quittiert das Wertübertragungszentrum den Erfolg der Übertragung ohne Anwendung kryptographischer Verfahren.

45 Deinstallation

[0141] Die Möglichkeit einer Deinstallation des Kundensystems muss durch den Kunden möglich sein.

[0142] Die detaillierte, technische Beschreibung der Schnittstelle Abrechnungsbetrag erfolgt mit Konzeption des post-eigenen Wertübertragungszentrums.

Nutzungsprotokoll und Nutzungsprofil

[0143] Im Kundensystem ist im Rahmen jeder Erzeugung eines Freimachungsvermerks ein Protokolleintrag zu erzeugen, der alle Angaben des jeweiligen Freimachungsvermerks – versehen mit einer digitalen Signatur des Sicherungsmoduls – enthalten muss. Weiterhin muss im Protokoll jeder Fehlerstatus des Sicherungsmoduls derart verzeichnet werden, dass die manuelle Löschung dieses Eintrags bei der Überprüfung bemerkt wird.

[0144] Das Nutzungsprofil enthält eine aufbereitete Zusammenfassung der Nutzungsdaten seit der letzten Kommunikation mit dem Wertübertragungszentrum.

[0145] Ist ein Kundensystem in eine beim Kunden befindliche und eine zentral (z. B. im Internet befindliche) Komponente aufgetrennt, so muss das Nutzungsprofil in der zentralen Komponente geführt werden.

Schnittstelle Freimachungsvermerk

65 Bestandteile und Ausprägungen

[0146] Das Kundensystem muss in der Lage sein, PC-Freimachungsvermerke zu erzeugen, die exakt den Vorgaben der Deutschen Post, beziehungsweise dem Rahmen der gängigen CEN- und UPU-Standards entsprechen.

[0147] PC-Freimachungsvermerke bestehen vorzugsweise aus folgenden drei Elementen:

- Einem 2-dimensionalen Strichcode, Barcode oder Matrixcode, in dem sendungsspezifische Informationen in maschinenlesbarer Form dargestellt sind. (Zweck: Automatisierung in der Produktion und Entgeltsicherung der Deutschen Post.)
- Text in Klarschrift, der wichtige Teile der Strichcode-Information in lesbarer Form wiedergibt. (Zweck: Kontrollmöglichkeit für den Kunden sowie in der Produktion und Entgeltsicherung der Deutschen Post.)
- Eine den Versendungsdienstleister, beispielsweise die Deutsche Post, kennzeichnende Marke wie beispielsweise ein Posthorn.

5

10

Spezifikation des Dateninhaltes

[0148] Zweckmäßigerweise enthalten Strichcode und Klartext des PC-Freimachungsvermerks folgende Informationen:

15

20

25

30

35

40

45

50

55

60

65

Tabelle

Inhalt des PC-Freimachungsvermerks

		Im Strich code	Im Klar- text		Größe (Byte)	Typ	Anmerkung
1	Post- Unternehmen	Ja	Nein		3	Binär	z.B. Deutsche Post
2	Freimachungs- art	Ja	Nein		1	Binär	z.B. PC-Frankierung
3	Version und Version Preis/Produkt	Ja	Nein		1	Binär	
4	Krypto- Algorithmus-ID	Ja	Nein		1	Binär	z.B. TDES, 128 bit
5	Ladevorgangs identifikati onsnummer (verschlüsselt) - Hersteller - Modell - Serien-Nr. - lfd. Vorgabe - Betrag - Währung - Gültig bis - Redundanz	Ja			16	Binär	
6	Zufallszahl (verschlüsselt)	Ja	Nein		16	Binär	
7	lfd. Sendungs- Nr.	Ja	Ja		3	Binär	bezogen auf das Sicherungsmodul
8a	Produktart	Ja	Ja		2	Binär	einschl. Zusatz- leistung - Im Klartext nur bei ermäßigten Sen- dungsarten (z.B. Infobrief)
8b	Versendungsform	Nein	Ja		-		Sendungsart bzw. gesonderte Ver- sendungsform
9	Entgelt	Ja	Ja		2	Binär	Klartext in ASCII
10	Freimachungs- datum	Ja	Ja		3	Binär	
11	PLZ des Empfängers	Ja	Nein		3	Binär	
12	Straße/Postfach des Empfängers	Ja	Nein		6	ASCII	Ersten und letzten drei Stellen der Anschrift
13	Restwert des Wertbetrages	Ja	Nein		3	Binär	
14	Hash-Wert	Ja	Nein		20	Binär	SHA-1

[0149] Beschrieben wird hier nur der Inhalt des Freimachungsvermerks. Die Vorschriften des Versendungsdienstleisters für den Inhalt der Adressangaben behalten unverändert ihre Gültigkeit.

Spezifikation der physikalischen Ausprägung auf Papier(Layout)

[0150] Der Freimachungsvermerk ist vorteilhafterweise im Anschriftenfeld linksbündig oberhalb der Anschrift auf der Sendung angebracht.

[0151] Das Anschriftenfeld wird in der jeweils gültigen Fassung der Normen des Versendungsdienstleisters spezifi-

zert. So werden insbesondere folgende Freimachungen ermöglicht:

- Aufdruck auf den Briefumschlag,
- Aufdruck auf Klebeetiketten oder
- Verwendung von Fensterbriefumschlägen derart, dass der Aufdruck auf den Brief durch das Fenster vollständig sichtbar ist.

[0152] Für die einzelnen Elemente des Freimachungsvermerks gilt vorzugsweise:

Verwendet wird zunächst der Strichcode vom Type Data Matrix, dessen einzelne Bildpunkte eine Kantenlänge von mindestens 0,5 Millimeter aufweisen sollten.

Im Hinblick auf lesetechnische Voraussetzungen sollte ein 2D-Barcode in Form der Data Matrix mit einer minimalen Pixelgröße von 0,5 mm bevorzugt zur Anwendung kommen. Eine ggf. zweckmäßige Option besteht darin, die Pixel-Größe auf 0,3 mm zu reduzieren.

Bei einer Darstellungsgröße von 0,5 mm pro Pixel ergibt sich eine Kantenlänge des gesamten Barcodes von ca. 18 bis 20 mm, wenn alle Daten wie beschrieben eingehen. Falls es gelingt, Barcodes mit einer Pixelgröße von 0,3 mm in der ALM zu lesen, lässt sich die Kantenlänge auf ca. 13 mm reduzieren.

Eine nachträgliche Erweiterung der Spezifikationen auf die Verwendung eines anderen Barcodes (z. B. Aztec) bei gleichen Dateninhalten ist möglich.

[0153] Eine bevorzugte Ausführungsform des Layouts und der Positionierung der einzelnen Elemente des Freimachungsvermerks ist nachfolgend in Fig. 5 beispielhaft dargestellt.

[0154] Die "kritischste" Größe ist die Höhe des dargestellten Fensters eines Fensterbriefumschlags mit einer Größe von 45 mm x 90 mm. Hier dargestellt wird ein DataMatrix-Code mit einer Kantenlänge von ca. 13 mm, der bei Verwendung der vorgeschlagenen Datenfelder nur bei einer Pixelauflösung von 0,3 mm möglich ist. Ein Code mit einer Kantenlänge von 24 mm lässt bezüglich der zur Verfügung stehenden Höhe keinen ausreichenden Raum für Angaben zur Anschrift.

Druckqualität und Lesbarkeit

[0155] Verantwortlich für den einwandfreien Aufdruck des Freimachungsvermerks sind der Hersteller des Kundensystems im Rahmen des Zulassungsverfahrens sowie der Kunde im späteren Betrieb. Hierzu ist der Kunde durch geeignete Hinweise in einem Benutzerhandbuch und einem Hilfesystem hinzuweisen. Dies gilt insbesondere für das saubere Haf-ten von Etiketten und das Verhindern des Verrutschens (von Teilen) des Freimachungsvermerks außerhalb des sichtbaren Bereichs von Fensterbriefumschlägen.

[0156] Die maschinelle Lesbarkeit von Freimachungsvermerken steht in Abhängigkeit von der verwendeten Druckauflösung und vom Kontrast. Sollen statt schwarz auch andere Farben zur Anwendung kommen, so ist mit einer geringeren Leserate zu rechnen. Es ist davon auszugehen, dass die geforderte Leserate bei einer im Drucker verwendeten Auflösung von 300 dpi ("dots per inch") bei hohem Druck-Kontrast gewährleistet werden kann; das entspricht etwa 120 Bildpunkten pro Zentimeter.

Testdrucke

40

[0157] Das Kundensystem muss in der Lage sein, Freimachungsvermerke zu produzieren, die in Ausprägung und Größe gültigen Freimachungsvermerken entsprechen, jedoch nicht für den Versand bestimmt sind, sondern für Kontrollausdrucke und der Drucker-Feinjustierung dienen.

[0158] Vorzugsweise ist das Kundensystem so gestaltet, dass die Testdrucke sich in einer für das Versendungsunternehmen erkennbaren Weise von tatsächlichen Freimachungsvermerken unterscheidet. Dazu wird beispielsweise in der Mitte des Freimachungsvermerks die Aufschrift "MUSTER – nicht versenden" angebracht. Mindestens zwei Drittel des Bar- codes, sollen durch die Aufschrift oder anderweitig unkenntlich gemacht werden.

[0159] Neben echten (bezahlten) Freimachungsvermerken dürfen außer gesondert gekennzeichneten Testdrucken keine Nulldrucke hergestellt werden.

45

50

Anforderungen an das Kundensystem

Basis-System

55

Überblick und Funktionalität

[0160] Das Basis-System dient als Bindeglied zwischen den anderen Komponenten der PC-Frankierung, namentlich dem Wertübertragungszentrum, des Sicherungsmoduls, dem Drucker und dem Kunden. Es besteht aus einem oder mehreren Computersystemen, zum Beispiel PCs, die ggf. auch durch ein Netzwerk miteinander verbunden sein können.

60

[0161] Eine Darstellung des Gesamtsystems ist in Fig. 6 dargestellt.

[0162] Das Basis-System stellt auch die komfortable Benutzung des Gesamtsystems durch den Kunden sicher.

Anforderungen an den Aufbau und die Sicherheit

65

[0163] Das Basis-System verfügt vorzugsweise über vier Schnittstellen:

1. Über die beschriebene Schnittstelle Abrechnungsbetrag erfolgt die Kommunikation mit dem Wertübertragungs-

zentrum.

2. Über eine Schnittstelle zum Sicherungsmodul werden alle Informationen ausgetauscht, die dem Sicherungsmodul bekanntgegeben werden müssen (Abrechnungsbetrag, beziehungsweise Ladevorgangsidentifikationsnummer, sendungsspezifische Daten zu einzelnen Frankierungen). Außerdem werden über diese Schnittstellen alle Daten mit dem Sicherungsmodul ausgetauscht (kryptographisch verarbeitete Daten).

3. Über eine Schnittstelle zum Drucker wird dieser angesteuert.

4. Über eine Schnittstelle zum Benutzer, beziehungsweise Kunden (Graphical User Interface, GUI), muss dieser alle relevanten Prozesse in Interaktion mit der größtmöglichen Ergonomie veranlassen können.

10 [0164] Im Basis-System sollten außerdem folgende Daten gespeichert und verarbeitet werden:

- Benutzerspezifische Einstellungen/Daten,
- detaillierte Nutzungsprotokolle und Nutzungsprofile,
- bei Verwendung von SSL: auswechselbare Zertifikate, mit denen die Gültigkeit der SSL-Zertifikate verifiziert werden können und
- alle relevanten Informationen über die Produkte und Preise des Versendungsdienstleisters.

Funktionsumfang und Abläufe

20 [0165] Das Basis-System unterstützt vorzugsweise folgende Abläufe:

- Erstinstallation mit Benutzerhilfe,
- Benutzeridentifikation, insbesondere gegenüber dem Sicherungsmodul; gegebenenfalls mit unterschiedlichen Berechtigungen für Laden von Abrechnungsbeträgen und Herstellung von Freimachungsvermerken,
- gegebenenfalls Administration mehrerer Benutzer,
- Unterstützung des Benutzers beim Laden von Abrechnungsbeträgen (hierbei Unterstützung der Wiedergabe von Informationen, die vom Wertübertragungszentrum in Form von HTML-kodierten Dateien gesandt werden),
- Unterstützung des Benutzers beim Auftreten von Problemen beim Laden von Abrechnungsbeträgen,
- für den Benutzer transparente Verwaltung des Wertbetrages (Kontoübersicht),
- Verwaltung von Nutzungsprotokollen, Aufbereitung von Nutzungsprofilen und Übertragung von Nutzungsprotokollen oder -profilen,
- Unterstützung des Benutzers bei der Erzeugung und beim Ausdruck des Freimachungsvermerks (Veranschaulichung eines Musters des zu druckenden Freimachungsvermerks auf dem Bildschirm – WYSIWYG),
- plausibilitätsgeprüfte Entgeltberechnung gemäß Service-Information der Deutschen Post,
- elektronisches Hilfesystem,
- automatische Aktualisierung der relevanten Informationen über die Produkte und Preise der Deutschen Post bei Änderungen sowie Information des Kunden über die stattfindende und abgeschlossene Aktualisierung,
- technische Unterbindung des mehrfachen Ausdrucks ein- und desselben Freimachungsvermerks und
- De-Installation des Kundensystems.

Sicherungsmodul

Aufgabe und Sicherheitsniveau

45 [0166] Das Sicherungsmodul gewährleistet als "kryptographisches Modul" im Sinne der FIPS PUB 140, Security Requirements for Cryptographic Modules, die eigentliche Sicherheit des Kundensystems. Sie besteht aus Hardware, Software, Firmware oder einer Kombination hieraus und beherbergt die kryptographische Logik und die kryptographischen Prozesse, das heißt, die Verwaltung und Anwendung kryptographischer Verfahren sowie die manipulationssichere Speicherung des Wertbetrages. Die Anforderungen, denen das Sicherungsmodul genügen muss, werden

- bezüglich des Sicherheitsstandards durch geeignete Normen, wie beispielsweise FIPS PUB 140 definiert und
- bezüglich der Einhaltung von Post-Standards durch die an FIPS PUB 140 angelehnte UPU-Veröffentlichung "International Postage Meter Approval Requirements (IPMAR)" definiert.

55 [0167] Zur Einführung und zum Betrieb in einem Kundensystem muss ein Sicherungsmodul als Kryptographisches Modul nach FIPS PUB 140 – vorzugsweise nach Sicherheitsstufe 3 (Security Level 3) – im Rahmen des Einführungsvorfahrens entsprechend zertifiziert werden.

Prozesse des Sicherungsmoduls

60 [0168] Das Sicherungsmodul sollte vorzugsweise zur Initialisierung und zur Kommunikation mit dem Wertübertragungszentrum und Deaktivierung neben üblichen Operationen im Wesentlichen folgende Prozesse unterstützen, die im hinteren Teil des Anhangs Technische Beschreibung Kundensystem detailliert beschrieben werden:

- Schlüsselerzeugung
- Ausgabe des öffentlichen Schlüssels

- Zertifikatspeicherung		
- Signaturerzeugung		
- Signaturprüfung		
- Zertifikatprüfung		
- Temporäre Zertifikatspeicherung		5
- Asymmetrische Verschlüsselung		
- Asymmetrische Entschlüsselung		
- Zufallszahlerzeugung		
- Speicherung eines Sitzungsschlüssels		
- Speicherung von zwei Ladevorgangsidentifikationsnummern		10
- Speicherung des aktuellen Registerwerts der Abrechnungsbeträge		
- Speicherung des aufsteigenden Registerwerts		
- Benutzeridentifikation		
- Statusausgabe der Gültigkeit der Abrechnungsbeträge		
- Statusausgabe des Registerwerts der Abrechnungsbeträge		15
- Hash-Bildung der sendungsspezifischen Daten		
- Verminderung der Registerwerte von geladenen Abrechnungsbeträgen		
- Fehlerprotokollierung		
- Selbsttest		
- Deaktivierung		20

Testdrucke

Das Sicherungsmodul wird beim Testdruck nicht verwendet und daher auch nicht kontaktiert. 25

Drucker

[0169] Der Drucker kann nach Massgabe des Herstellers des Kundensystems entweder ein handelsüblicher Standarddrucker oder ein Spezialdrucker sein. 30

[0170] Die große Mehrzahl heutiger Laser- und Tintenstrahldrucker sollte prinzipiell für die PC-Frankierung geeignet sein. Empfohlen werden sollten Drucker mit einer Auflösung von wenigstens 300 dpi (dots per inch).

Prozesse innerhalb des Kundensystems

35

Ablauf der Erzeugung von Freimachungsvermerken

[0171] Durch das Kundensystem führt der Kunde folgende Teilprozesse bei der Erzeugung von Freimachungsvermerken durch:

40

- Aufbau der Verbindung zum Sicherungsmodul: Über das Basis-System wird eine Verbindung zum Sicherungsmodul hergestellt.
- Identifikation des Benutzers: Der Benutzer identifiziert sich mit Passwort/PIN persönlich bei dem Sicherungsmodul und aktiviert diese somit.
- Eingabe der sendungsspezifischen Informationen: Der Kunde gibt, mit Unterstützung des Kundensystems, die erforderlichen sendungsspezifischen Informationen in das Basis-System ein, das die wesentlichen Daten an das Sicherungsmodul übergibt.
- Erzeugung des Freimachungsvermerks: Das Basis-System erzeugt aus den sendungsspezifischen Daten und den kryptographisch verarbeiteten Daten aus dem Sicherungsmodul einen Freimachungsvermerk.
- Protokollierung der Herstellung von Freimachungsvermerken: 50

Jede erfolgreiche Rückübertragung wird in einem Nutzungsprotokoll des Basis-Systems festgehalten. Bei einer Aufteilung des Kundensystems in eine lokale Komponente beim Kunden und eine zentrale Komponente (z. B. im Internet) ist das Nutzungsprotokoll in der zentralen Komponente zu führen.

- Abbau der Kommunikationsbeziehung: Sind alle angeforderten Freimachungsvermerke hergestellt worden, so wird die Kommunikationsbeziehung wieder abgebaut. Bei erneuter Herstellung von Freimachungsvermerken ist die Benutzeridentifikation wieder – wie oben beschrieben – vorzunehmen.
- Testdrucke: Alternativ zu dieser Vorgehensweise ist es möglich, die Benutzerführung so weit forschreiten zu lassen, dass ein Muster eines Freimachungsvermerks sowohl auf dem Bildschirm dargestellt (WYSIWYG) als auch als (nicht gültiger) Testdruck ausgedruckt werden kann. Erst in einem späten Stadium würde hierbei der oben genannte Prozess der Einbeziehung des Sicherungsmoduls erfolgen. 55

[0172] Der Einsatz des technischen Systems wird durch zweckmäßige organisatorische Maßnahmen flankiert, so dass ein technisch registrierbarer Mehrfachversand eines Freimachungsvermerkes auch als ein Verstoß gegen Geschäftsbedingungen des Versenders betrachtet wird.

60

[0173] Ferner ist es vorteilhaft, geeignete technische Parameter für den Ausdruck der Freimachungsvermerke vorzusehen, insbesondere bezüglich der Druckqualität, damit die Freimachungsvermerke in automatischen Erfassungseinrichtungen besser erfasst werden können.

65

[0174] Für eine Überprüfung der Systeme können geeignete Qualitätssicherungssysteme, insbesondere nach den Nor-

men ISO 9001 ff. zugrunde gelegt werden.

Patentansprüche

5. 1. Verfahren zum Versehen von Postsendungen mit Freimachungsvermerken, wobei ein Kundensystem von einem Wertübertragungszentrum über eine Datenleitung einen Gebührenbetrag lädt, wobei das Kundensystem ein Drucken von Freimachungsvermerken auf Postsendungen steuert und wobei das Wertübertragungszentrum ein Datenpaket an das Kundensystem sendet, dadurch gekennzeichnet, dass in dem Kundensystem Daten erzeugt werden, die so verschlüsselt sind, dass das Wertübertragungszentrum diese entschlüsseln kann, dass die Daten von dem Kundensystem zu dem Wertübertragungszentrum gesendet werden und dass das Wertübertragungszentrum die Daten entschlüsselt und anschließend die Daten erneut mit einem dem Kundensystem nicht bekannten Schlüssel verschlüsselt und die so verschlüsselten Daten anschließend an das Kundensystem überträgt.

10. 2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Verschlüsselung in dem Kundensystem unter Einsatz einer Zufallszahl erfolgt.

15. 3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die Zufallszahl in einem Sicherungsmodul erzeugt wird, auf das ein Benutzer des Kundensystems keinen Zugriff hat.

4. Verfahren nach einem oder beiden der Ansprüche 2 oder 3, dadurch gekennzeichnet, dass die Zufallszahl zusammen mit einem von dem Wertübertragungszentrum ausgegebenen Sitzungsschlüssel und einem öffentlichen Schlüssel des Wertübertragungszentrums verschlüsselt wird.

20. 5. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass das Kundensystem die Daten mit einem privaten Schlüssel signiert.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass der private Schlüssel in dem Sicherungsmodul gespeichert ist.

7. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass die Daten mit jeder Anforderung eines Gebührenbetrages von dem Kundensystem an das Wertübertragungszentrum übertragen werden.

25. 8. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass das Wertübertragungszentrum anhand der übermittelten Daten das Kundensystem identifiziert.

9. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass das Wertübertragungszentrum die von ihm verschlüsselten Daten an das Kundensystem schickt.

30. 10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass die von dem Wertübertragungszentrum an das Kundensystem gesandten Daten einen ersten Bestandteil aufweisen, der von dem Kundensystem nicht entschlüsselt werden kann und dass die Daten ferner einen zweiten Anteil aufweisen, der von dem Kundensystem entschlüsselt werden kann.

35. 11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass der in dem vom Kundensystem entschlüsselbare Teil der Daten Informationen über die Identität des Kundensystems enthält.

12. Verfahren nach einem oder beiden der Ansprüche 10 oder 11, dadurch gekennzeichnet, dass der von dem Kundensystem entschlüsselbare Anteil der Daten Informationen über die Höhe eines Gebührenbetrages enthält.

40. 13. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass bei jeder Datenübertragung von dem Wertübertragungszentrum zu dem Kundensystem ein Betrag übertragen wird, der zur Erstellung von mehreren Freimachungsvermerken ausreicht.

14. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass in dem Kundensystem ein Hash-Wert gebildet wird.

45. 15. Verfahren nach Anspruch 14, dadurch gekennzeichnet, dass der Hash-Wert unter Einbeziehung von Angaben über Sendungsdaten gebildet wird.

16. Verfahren nach einem oder mehreren der Ansprüche 14 oder 15, dadurch gekennzeichnet, dass der Hash-Wert unter Einbeziehung einer zwischengespeicherten Zufallszahl gebildet wird.

17. Verfahren nach einem oder mehreren der Ansprüche 14 bis 16, dadurch gekennzeichnet, dass der Hash-Wert unter Einbeziehung einer Ladevorgangsidentifikationsnummer gebildet wird.

50. 18. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass der Freimachungsvermerk logische Daten enthält.

19. Verfahren nach Anspruch 18, dadurch gekennzeichnet, dass der Freimachungsvermerk Informationen über Sendungsdaten enthält.

20. Verfahren nach einem oder beiden der Ansprüche 18 oder 19, dadurch gekennzeichnet, dass die logischen Daten Informationen über die verschlüsselte Zufallszahl enthalten.

55. 21. Verfahren nach einem oder mehreren der Ansprüche 18 bis 20, dadurch gekennzeichnet, dass die logischen Daten Informationen über die verschlüsselte Ladevorgangsidentifikationsnummer enthalten.

22. Verfahren nach einem oder mehreren der Ansprüche 18 bis 21, dadurch gekennzeichnet, dass die logischen Daten Informationen über den Hash-Wert enthalten.

60. 23. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass der Freimachungsvermerk sowohl von dem Wertübertragungszentrum übertragene Informationen als auch von dem Dokumentenhersteller eingegebene Daten enthält.

24. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass der Freimachungsvermerk einen Hash-Wert enthält, der aus einer Kombination aus einem von dem Vorgabezentrum übertragenen Wert und von dem Dokumentenhersteller eingegebenen Wert gebildet wird.

65. 25. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass es folgende Verfahrensschritte beinhaltet: In dem Kundensystem oder in einem mit dem Kundensystem verbundenen Sicherungsmodul wird ein Geheimnis erzeugt und anschließend zusammen mit Informationen über die Identität des

Dokumentherstellers und/oder des von ihm eingesetzten Kundensystems an das Wertübertragungszentrum übermittelt.	
26. Verfahren nach Anspruch 25, dadurch gekennzeichnet, dass das Wertübertragungszentrum die verschlüsselte Zusatzzahl entschlüsselt und anschliessend eine Ladeidentifikationsnummer erzeugt.	5
27. Verfahren nach Anspruch 26, dadurch gekennzeichnet, dass bei der Erzeugung der Ladeidentifikationsnummer die entschlüsselte Zufallszahl eingeht.	
28. Verfahren nach Anspruch 26 oder 27, dadurch gekennzeichnet, dass die Ladeidentifikationsnummer an das Sicherungsmodul übertragen wird.	10
29. Verfahren nach Anspruch 28, dadurch gekennzeichnet, dass in dem Sicherungsmodul ein Hash-Wert aus der Ladeidentifikationsnummer und weiteren Daten gebildet wird.	
30. Verfahren nach Anspruch 28, dadurch gekennzeichnet, dass der Freimachungsvermerk so erzeugt wird, dass er den Hash-Wert enthält.	
31. Verfahren nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass die Gültigkeit von Freimachungsvermerken in dem Briefzentrum überprüft wird.	15
32. Verfahren nach Anspruch 28, dadurch gekennzeichnet, dass die Prüfung in dem Briefzentrum durch eine Analyse von in dem Freimachungsvermerk enthaltenen Daten erfolgt.	
33. Verfahren nach einem oder beiden der Ansprüche 31 oder 32, dadurch gekennzeichnet, dass die Prüfungsstelle aus in dem Freimachungsvermerk enthaltenen Daten einen Hash-Wert bildet und überprüft, ob dieser Hash-Wert mit einem in dem Freimachungsvermerk enthaltenen Hash-Wert übereinstimmt und im Falle der Nichtübereinstimmung den Freimachungsvermerk als gefälscht registriert.	20
34. Kundensystem zur Frankierung von Postsendungen, dadurch gekennzeichnet, dass es Mittel für eine Verschlüsselung von Daten enthält, dass es einen Datenausgang für eine Ausgabe der verschlüsselten Daten an ein Wertübertragungszentrum enthält und dass es einen Dateneingang für einen Empfang von durch das Wertübertragungszentrum anders verschlüsselte Daten enthält und dass das Sicherungsmodul so gestaltet ist, dass es die von dem Wertübertragungszentrum empfangenen Daten nicht vollständig entschlüsseln kann.	
35. Wertübertragungszentrum für den Einsatz in einem Verfahren nach einem oder mehreren der Ansprüche 1 bis 33, dadurch gekennzeichnet, dass es einen Dateneingang enthält, wobei durch den Dateneingang von Kundensystemen gesandte verschlüsselte Daten in das Wertübertragungszentrum gelangen, mit Mitteln zur Entschlüsselung der empfangenen Daten und mit Mitteln zu einer erneuten Verschlüsselung der Daten, wobei das Mittel zur Verschlüsselung der Daten so beschaffen ist, dass es die Daten anders verschlüsselt als sie von dem Wertübertragungszentrum empfangen wurden.	25
	30

Hierzu 4 Seite(n) Zeichnungen

35

40

45

50

55

60

65

- Leerseite -

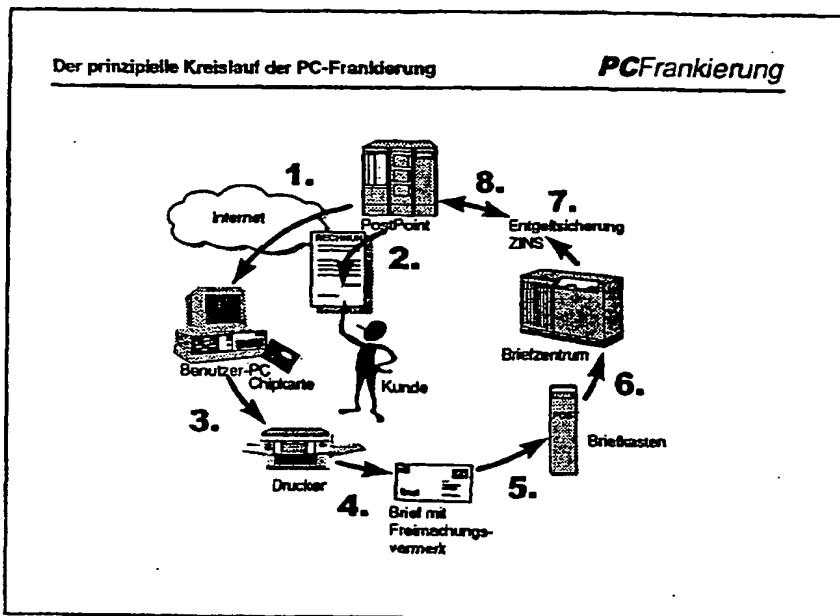


Abbildung 1

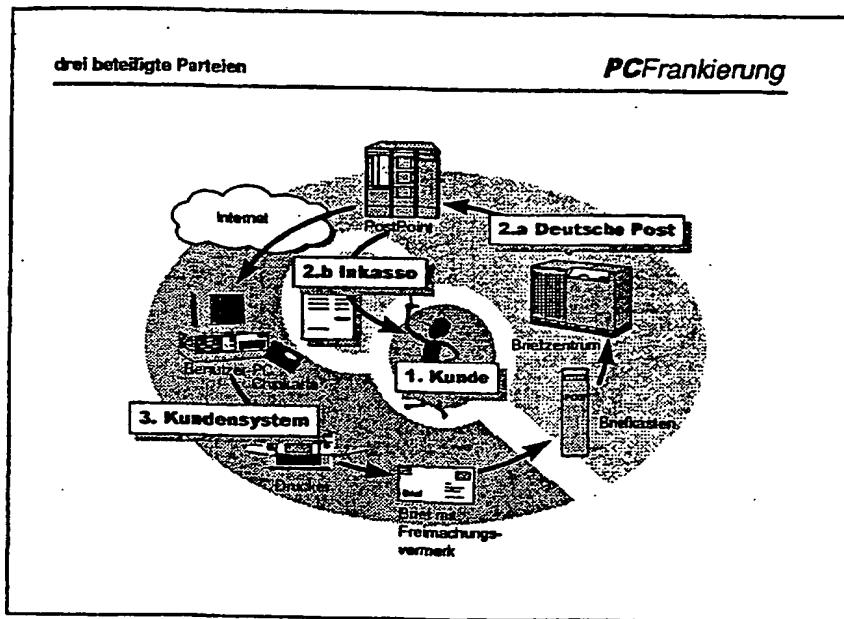


Abbildung 2

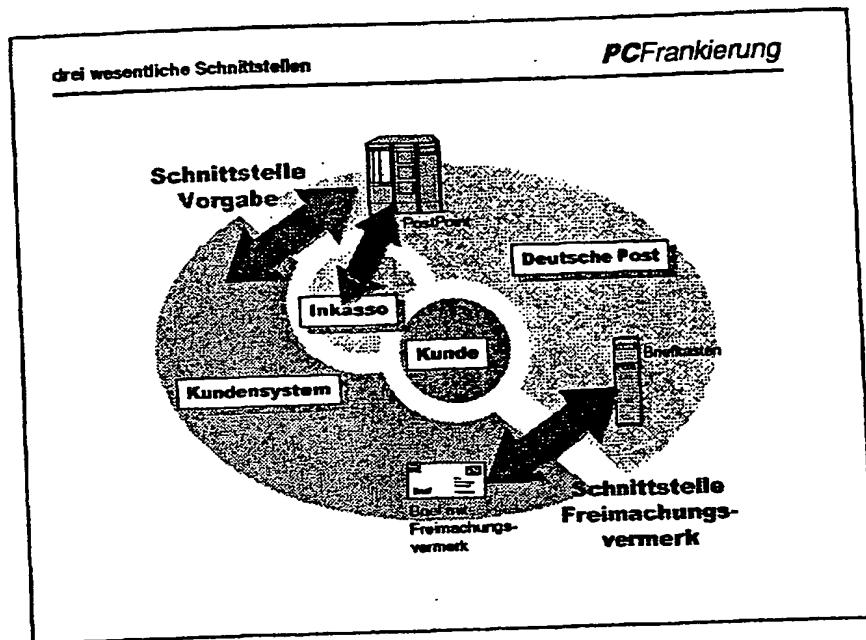


Abbildung 3

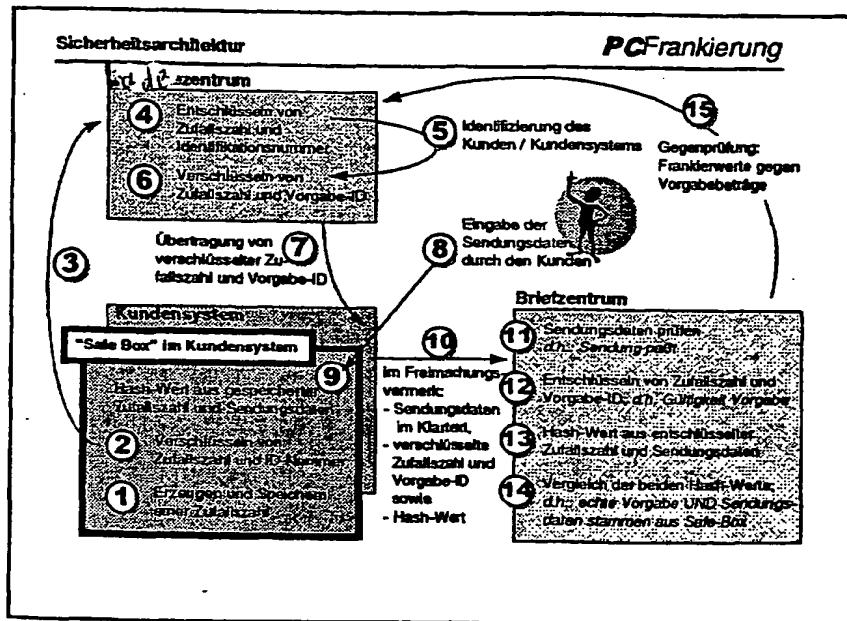


Abbildung 4

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.